Technical overview of public XSEDE authentication services

Version 1.1
June 29, 2017

This is a technical overview of the public authentication services that XSEDE offers and the specific features each offers. This document offers more detail than is provided by the standard XSEDE documentation.

Purpose

Science gateways that use XSEDE services are required to report on the number of researchers who use them, and--in certain situations, notably, security incidents--to be able to provide information about specific users and their activities within the gateway. Gateway developers and operators may use any method they like to do this, but XSEDE provides services intended to make this task easier.

XSEDE's authentication service [10] is an option available to gateway developers and operators. It provides a "login" user interface that the gateway can present to its users. It provides the gateway with a specific, authenticated user identity that the gateway can then use for tracking use and authorizing access to specific gateway features. This service offer several benefits to gateway developers, gateway operators, and gateway users.

- It relieves the gateway developer and operator from managing a user database.
- It simplifies the code required for user authentication in the gateway.
- It helps XSEDE and gateway developers jointly maintain a consistent level of quality in our security interfaces.
- It enables researchers to use existing identities (their campus credentials, for example) to login to the gateway instead of setting up brand-new identities.
- Existing identities (e.g., campus credentials) are generally more reliable than identities established solely for use with a gateway, so encouraging their use improves our overall security.
- When researchers use existing identities to authenticate to a gateway, it helps us (and our sponsors) understand the relationship between people who use the gateway and people who use other services (other gateways, XSEDE services, campus services).

This document describes XSEDE's authentication service and provides references for getting started using it. This is not the "how to" documentation, however! Please use the references provided to learn how to use XSEDE's authentication service in a science gateway.

XSEDE's authentication service

In 2016, XSEDE began offering a public authentication service based on the popular OAuth 2.0 [1] and OpenID Connect 1.0 [2] interfaces. This service allows other services (including science gateways) to register and authenticate users without maintaining a local user database or writing significant code. It supports the InCommon federation to which many academic and research organizations belong, and it also supports identities issued by other major research service providers, including NERSC/DOE, NIH, Google, and ORCID. Client SDKs and APIs are public, open source, and used and supported by a wide community of developers. XSEDE itself uses this service for the XSEDE User Portal (XUP).

XSEDE's authentication service is provided by Globus Auth [3], one of several services offered by Globus at the University of Chicago. In combination with a few supporting services, Globus Auth and XSEDE are able to offer user authentication services to science gateways, campuses, XSEDE and other service providers.

Globus Auth and XSEDE

Globus Auth is the primary authentication interface offered by XSEDE for use by external services. Globus Auth provides the ability to authenticate individual identities. A familiar way to think of this is as a "Login with X" service (think: "Login with Google" or "Login with Facebook"), where "X" can be any of several hundred academic and research organizations and public services. (Google is also supported.) An important "X" is, of course, XSEDE itself, which has a registered user community of more than 20,000 individuals who have used XSEDE services (and their predecessors) directly. Another 30-40,000 individuals use Globus via other organizations, which means that more than 50,000 individuals can already authenticate with Globus Auth without re-registering. New registrations are very easy for researchers, and usually involve linking to an existing campus user identity. XSEDE requests additional information--particularly for individuals who are not at participating institutions--but science gateways are not required to collect this information.

Science gateways can use Globus Auth at no cost, but registration is required. Most gateways will be able to use Globus Auth's free services for as long as the gateway needs them and will not need to use any of the additional supporting services offered by XSEDE. However, for gateways with specialized needs, both XSEDE and Globus offer further services.

Documentation on how to use Globus Auth is available online. [4] The service is operated and supported by the University of Chicago. University of Chicago is an XSEDE partner and an XSEDE service provider. Funding for Globus is provided by subscriptions from colleges, universities, and major research service providers, and in part by federal grant funding. Globus's services are not dependent on XSEDE for ongoing support.

Other supporting services

Globus Auth supports applications and gateways that are able to use an OAuth 2.0 (OAuth2) or OpenID Connect 1.0 (OIDC) mechanism. Most development frameworks, and even many public applications, have OAuth2 or OIDC "plugins," modules, or libraries that can be easily imported to support Globus Auth. For applications with more specialized needs, XSEDE provides supporting services to handle specialized needs that Globus Auth does not support directly. All of these are available for use by research applications and gateways at no cost.

- One of these is idp.xsede.org [6], which is an InCommon identity provider for XSEDE, supporting the SAML authentication interface used in the InCommon federation. [5] Applications and gateways that already work with InCommon's SAML-based mechanism can use idp.xsede.org to authenticate individuals who have registered with XSEDE.
- Another is OAuth for MyProxy (OA4MP) [7], which offers X.509 certificates for researchers who have registered with XSEDE. Applications and science gateways that specifically require X.509 certificates (presumably because they use other services that only support X.509) can use OA4MP.
- Finally, XSEDE and Globus Auth both use the CILogon service [8], provided by the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign, to allow Globus Auth to work with the InCommon federation. Applications and gateways do not need to use CILogon directly because it is already integrated with Globus Auth, but users at InCommon organizations will see CILogon when they authenticate with Globus Auth.

Globus Auth itself also offers specialized services via a subscription model. Most science gateways will not need these services as they are intended for research institutions or large research service providers.

- Applications that must provide a seamless user interface--with their own "look and feel" and Internet domain throughout the entire login process--can be supported via a subscription.
- Applications that need to support an existing user database that isn't already accessible via InCommon, OAuth2, or OIDC can be supported with a subscription.

Get started

To get started using XSEDE's authentication service in a science gateway or other application, you will first need to identify the specific development or portal framework you are using in your Gateway, or possibly the development language it uses. Then, search the documentation for your framework (or search the Web) to find an existing OIDC or OAuth2 plugin, module, or library that you can use. If you do not find a way to support OIDC or OAuth2 in your web application, look for one for the programming language you are developing in.

In many cases, you won't need to write any code yourself and will merely need to add OIDC or OAuth2 support to your web application, register it with Globus Auth to obtain client credentials, and configure it

to use Globus Auth and the credentials you received. These steps are described and documented in the Globus Auth documentation.

If neither OIDC nor OAuth2 are supported but InCommon/SAML/Shibboleth or X.509 are, see the section above on supporting services to identify the service offering that interface. Instructions for using these services are available on their websites.

Finally, if you have questions or need help with the instructions provided in these references, contact us at help@xsede.org.

Supporting interfaces

XSEDE's authentication service is supported by several authentication services. All of these services provide a login interface and all of them provide their clients with a specific user identity. The services are distinguished technically by their specific features, the identity providers (IDPs) they recognize, the authentication protocols they support, and the credential types they offer. (Globus Auth is XSEDE's primary authentication service. The others play supporting roles and are either used with the Globus Auth service or are provided to satisfy specialized needs.) The subsections below explain each of these characteristics in more detail. Table 1 provides a summary of the authentication services provided by XSEDE and their features.

	Globus Auth	**CILogon**	**OIDC/OAuth2 for MyProxy**	**idp.xsede.org**
Specific authentication features				
Can authenticate people who haven't registered with XSEDE?	yes	yes	no	no
Can authenticate people who don't have a current XSEDE allocation?	yes	yes	no	yes
Customizable login interface	yes*	yes	no	yes
Gateway must be registered to use the service?	yes	yes	yes	yes
Gateway can require a specific IDP (e.g., XSEDE)?	yes	yes	Must be XSEDE	Must be XSEDE
User registration (signup) included?	yes	no	no	yes
Supported identity providers (IDPs)				
XSEDE	yes	yes	yes	yes
InCommon (campuses)	yes	yes	no	no
Google	yes	yes	no	no
Globus ID	yes	no	no	no
GitHub	no	yes	no	no
ORCiD	yes	no**	no	no
Supported authentication protocols				
OAuth 2.0	yes	yes	yes	no
OAuth 1.0	yes	yes	yes	no
OpenID Connect (OIDC)	yes	yes	yes	no
SAML Single Sign-0n (SSO)	no	no**	no	yes
SAML Enhanced Client or Proxy (ECP)	no	yes	no	yes
Available credential types				
OAuth token	yes	yes	no	no
SAML assertion	no	no**	no	yes
X.509 certificate	no	yes	yes	no
* this feature requires a paid subscription ** this feature is planned for a future release of the service				

Table 1. Summary of XSEDE authentication services for science gateways

Table 2 provides references for information on how to access and use each of the services mentioned above.

Authentication service	Documentation
Globus Auth	https://docs.globus.org/api/auth/
CILogon	http://www.cilogon.org/oidc
OIDC/OAuth2 for MyProxy	https://oa4mp.xsede.org/oauth2/
idp.xsede.org	https://www.xsede.org/security/incommon

Table 2. Documentation sources for XSEDE authentication services

Specific authentication features

In addition to providing a basic login interface and returning an authenticated identity to the science gateway, each authentication service provides a different set of specific features. Table 1 provides a summary of each service's features, and the explanations below provide more detail on each feature.

XSEDE identity status

The status of the gateway user's relationship with XSEDE is treated differently by different services. Some services will only authenticate people who are known to XSEDE; that is, people who have registered with the XSEDE user portal and established an XSEDE username and password. Some services go further and will only authenticate people who currently have active XSEDE allocations (people who are members of a research project that is currently authorized to use specific XSEDE resources). Some services do not require any relationship with XSEDE at all, and will authenticate people based on other affiliations, such as campuses or research organizations, and/or allow people to establish brand new identities.

Customizable login interface

All external authentication services provide a basic login interface that can be incorporated into the science gateway so that people can "login" to the gateway. The degree to which this interface can be customized in appearance and functionality varies, however. Most login interfaces can be embedded within a gateway's interface so that it doesn't completely "take over" the user's browser window. Some allow the gateway to "skin" the interface, changing the styles and graphical elements within the login interface while retaining its functionality.

Gateway registration

Some external authentication services require that the science gateway register with the authentication service in order to use the service. This registration is performed by the gateway operator (or developer) and it tells the authorization service provider a bit about the gateway. This information is used to customize user interfaces and to prohibit unauthorized or malicious use of the service. Registration *does not* imply that payment is required: in fact, most registration services are free.

Required identity provider

Some authentication services allow science gateways to require that their users must be registered with a specific IDP (XSEDE, for example) in order to login. Typically, the authentication service will then always return the user's identity from the required provider, rather than any identities he/she may have with other providers. *This doesn't necessarily mean that the gateway user must authenticate with the required IDP every time he/she logs in.* The authentication service might allow users to securely *link* their identities from multiple providers, so that they can login using one provider (e.g., their campus) while the gateway is given the identity associated with the required provider (e.g., XSEDE).

User registration interface

All external authentication service rely on identities that have already been set up with one or more IDPs: XSEDE, the user's home institution, Google, etc. Some services, however, can guide the user who is attempting to login to the registration process for an IDP if he/she isn't already registered. (For example, the interface may allow the user to create a new account with XSEDE if he/she doesn't already have one.) Some services can even allow users to register with the authentication service itself (i.e., create a brand new identity) if they don't have (or don't choose to use) another organization that can serve as their IDP.

Supported identity providers

External authentication services typically allow end users (people who login to a gateway) to choose an IDP with whom they already have an established relationship. The authentication service allows the user to login to their IDP, and the service then receives identity information from the IDP, which it, in turn, delivers to the gateway.

Some authentication services use only a single IDP (e.g., XSEDE), requiring that the user must have an identity established with that IDP. Other services allow users to choose from a set of IDPs, unique to each service. The set of supported IDPs might include XSEDE, other national-scale service providers like NIH or DOE, individual college or university campuses, research laboratories, commercial or public service providers, and so on. Each authentication service supports a specific set of IDPs, and the set may change over time according to the service's rules of operation. Some services allow specific gateways to require a specific IDP (see "Required identity provider," above), but it must be within the set supported by the service.

Supported authentication protocols

The specific manner in which a science gateway interacts with an authentication service is determined by the authentication protocols offered by the service. Software libraries and extensions for web development frameworks are available for each protocol. (Use the protocol name to search for relevant extensions and libraries for the framework you are using.) Each protocol provides a specific set of features that the gateway can use to customize the login experience for its users.

OAuth 1.0 and 2.0

OAuth is technically an *authorization* protocol that allows users of one service (e.g., XSEDE) to authorize other services (e.g., a science gateway) to access their identity information from the first service. This mechanism is used by companies such as Google, Facebook, Microsoft and Twitter to permit their users to share information about their accounts with third party applications or websites. OAuth was designed specifically to work with Web browser-based services. [1] Via Globus and CILogon, campuses that participate in the InCommon federation can be used as OAuth 2.0 IDPs.

From the gateway developer's perspective, the user login process works as follows. First, the gateway will request an access token from an IDP. This results in the user's web browser being redirected to the IDP's login interface. (Note that IDPs often use browser cookies to "remember" users between login session, meaning that the user might not need to re-enter their username and password to login.) On successful login, the browser is returned to the gateway with an access token. The access token, in turn, allows the gateway to access the user's identity information from the IDP. The gateway now has the user's identity information and can use it to establish a local identity in the gateway (if the user doesn't already have one) and start the user's login session.

OpenID Connect (OIDC)

OIDC is an identity interface built on the OAuth 2.0 protocol that allows services to obtain someone's identity via OAuth 2.0 and then access additional profile information if desired. OIDC is a RESTful API that uses JSON as a data format. [2] OIDC is commonly used by Google, Microsoft, and many other commercial services. Via Globus and CILogon, campuses that participate in the InCommon federation may be used as OIDC IDPs.

SAML Single Sign-on (SSO)

SAML is a standard XML-based data format for exchanging authentication and authorization data between an IDP and a service provider. SAML is a product of the OASIS Security Services Technical Committee. SAML specifies a format for *assertions*: messages that assert identity information that can be passed from an IDP to a service provider. [5]

When someone wants to login to a science gateway, the gateway requests an *identity assertion* from an IDP. Before delivering the assertion, the IDP may request some information from the user--such as a username and password. (Often, however, the request to the IDP will include a web cookie set by a previous authentication, so the user won't need to re-enter their username and password.) The assertion returned from the IDP *may or may not* provide any specific details about the user. The gateway uses the assertion returned by the IDP to decide whether or not to establish a login session for the user.

SAML Enhanced Client or Proxy (ECP)

ECP is a SAML 2.0 profile that enables the exchange of SAML attributes outside the context of a web browser. ECP is useful for non-browser (command-line or "thick client") applications. Via CILogon, science gateways can fetch X.509 certificates for their users for any InCommon-member ECP-enabled IdP. [9] Some XSEDE service interfaces (GridFTP, GSI-SSH) accept X.509 certificates for authentication.

References

[1] https://en.wikipedia.org/wiki/OAuth

[2] https://openid.net/connect/

[3] S. Tuecke et al., "Globus auth: A research identity and access management platform," 2016 IEEE 12th International Conference on e-Science (e-Science), Baltimore, MD, 2016, pp. 203-212. DOI=10.1109/eScience.2016.7870901. (https://www.globus.org/sites/default/files/GlobusAuth.pdf)

[4] https://docs.globus.org/api/auth/

[5] https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

[6] https://www.xsede.org/security/incommon

[7] http://grid.ncsa.illinois.edu/myproxy/oauth/

[8] http://www.cilogon.org/

[9] http://www.cilogon.org/ecp

[10] “User authentication service for XSEDE science gateways.” Technical report, version 1.1, May 10, 2017. ()